PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 102, Number 3, March 1988

ON A CONJECTURE OF GRAHAM

J. W. SANDER

(Communicated by Larry T. Goldstein)

ABSTRACT. Let $a_1 < a_2 < \cdots < a_n$ be a finite sequence of positive integers containing a prime power p^d with the property: $a_i \neq p^k a_j$ for all i, j and $k > 0$. Then $\max_{i,j} a_i/(a_i, a_j) \geq n$.

In [4] R. L. Graham asks if the following is true: Let $\mathcal{A}$ be a finite sequence of n positive integers $a_1 < a_2 < \cdots < a_n$. Then $\max_{i,j} a_i/(a_i, a_j) \geq n$.

Several partial results have been obtained (see the references), particularly for the case where one of the a_i's is prime. The proofs for the latter follow similar lines, E. Z. Chein [2] and R. Klein [5] use G. Weinstein's improvement [9] upon R. Winterle's earlier result [10] while R. J. Simpson [7] can do without. In this paper we use refinements of the methods of Winterle [10] and Klein [5] to prove the following theorem. The sequence $\mathcal{A}$ is said to be p-simple for a prime p if $a_i \neq p^k a_j$ for $1 \leq i, j \leq n$, $k > 0$.

THEOREM. *Let $\mathcal{A}$ be p-simple for a prime $p \neq 2$ and let $\mathcal{A}$ contain a prime power $a_k = p^d$ $(d \geq 0)$. Then*

$$\max_{1 \leq i,j \leq n} \frac{a_i}{(a_i, a_j)} \geq n.$$

In order to prove the theorem we first consider the case where a_1 is the required prime power. For a given sequence $\mathcal{A}$ let $A = \{a_1, \ldots, a_n\}$.

LEMMA. *Let $\mathcal{A}$ be p-simple with $a_1 = p^d$ $(d \geq 0)$. Then*

$$\max_{i,j} \frac{a_i}{(a_i, a_j)} \geq n.$$

PROOF. We may assume $d > 0$, since the lemma is trivial for $a_1 = 1$. We suppose

$$\max_{i,j} \frac{a_i}{(a_i, a_j)} \leq n - 1. \tag{1}$$

This implies

$$a_n \leq (n-1)(a_n, a_1) \leq (n-1)p^d. \tag{2}$$

For $k = 0, 1, \ldots, d-1$ define

$$B_k = \{a_i \in A \colon p^k \| a_i\}, \quad \text{and} \quad B = A \setminus \bigcup_{k=0}^{d-1} B_k.$$

Received by the editors July 18, 1986 and, in revised form, November 5, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 10A05; Secondary 02A05.

Furthermore, for $k = 0, 1, \ldots, d-1$ and each $a_i \in B_k$ define

$$T_k(a_i) = p^{h_{i,k}}(a_i - p^{k+1}) \tag{3}$$

such that $h_{i,k}$ is maximal with

$$T_k(a_i) \leq (n-1)p^d. \tag{4}$$

Obviously, $T_k(a_i) > 0$ and the maximality of $h_{i,k}$ gives

$$T_k(a_i) > (n-1)p^{d-1}. \tag{5}$$

We have for $a_i \in B_k$

$$a_i \leq (n-1)p^k; \tag{6}$$

otherwise $a_i = p^k a_i'$ with $a_i' \geq n$, $p \nmid a_i'$. This yields $a_i/(a_i, a_1) = p^k a_i'/p^k = a_i' \geq n$ which contradicts (1). By (3), (4) and (6) we have $h_{i,k} \geq d-k$ which implies

$$p^d | T_k(a_i). \tag{7}$$

Since $(a_i, a_i - p^{k+1}) = (a_i, p^{k+1}) = p^k$ for $a_i \in B_k$, we get

$$(a_i, T_k(a_i)) = p^k. \tag{8}$$

We claim for $a_i \in B_k$, $a_j \in B$,

$$T_k(a_i) \neq a_j; \tag{9}$$

otherwise by (5) and (8)

$$a_j/(a_j, a_i) = T_k(a_i)/(T_k(a_i), a_i) > n-1$$

which contradicts (1).

We claim for $a_i \in B_{k_1}$, $a_j \in B_{k_2}$, $a_i \neq a_j$,

$$T_{k_1}(a_i) \neq T_{k_2}(a_j); \tag{10}$$

otherwise

$$p^{h_{i,k_1}}(a_i - p^{k_1+1}) = p^{h_{j,k_2}}(a_j - p^{k_2+1}),$$

hence

$$a_i/p^{k_1} - p = a_j/p^{k_2} - p$$

which contradicts the p-simplicity of $\mathcal{A}$.

Now define the following function $F\colon A \to \mathbf{N}$ by

$$F(a_i) = \begin{cases} T_k(a_i) & \text{for } a_i \in B_k, \\ a_i & \text{for } a_i \in B. \end{cases}$$

By (9) and (10) F is 1-1. By (2), (4) and (7) we have for all $i = 1, \ldots, n$

$$0 < F(a_i) \leq (n-1)p^d \quad \text{and} \quad p^d | F(a_i).$$

This contradiction proves the lemma.

PROOF OF THE THEOREM. We may assume that $\mathcal{A}$ is proper, i.e. the g.c.d. of the a_i's is 1. We may also assume that p^d is the lowest p-power in A and $d > 0$. We suppose

$$\max_{i,j} \frac{a_i}{(a_i, a_j)} \leq n-1. \tag{11}$$

Define $B_0 = \{1, 2, \ldots, n-1\} \backslash \{p, p^2, \ldots, p^{d-1}\}$ and $B_d = \{lp^d \colon \lceil n/p^d \rceil \le l \le n-2\}$; for $h = 1, 2, \ldots, d-1$ let

$$B_h = \{lp^h \colon \lceil n/p^h \rceil \le l \le n-1, (l,p) = 1\}.$$

Obviously, $B_0, \ldots, B_d$ are pairwise disjoint.

We claim

$$A \subseteq \bigcup_{h=0}^{d} B_h; \tag{12}$$

therefore, let $a_i \in A$. If $a_i \le n-1$ then $a_i \in B_0$ since p^d is the lowest p-power in A. If $a_i \ge n$ then $p | a_i$, for otherwise $a_i/(a_i, a_k) = a_i/(a_i, p^d) = a_i \ge n$, contradicting (11). Now we distinguish between two cases:

Case 1. $p^h \| a_i$ for some h, $1 \le h \le d-1$. Then $a_i = p^h a_i'$, $(a_i', p) = 1$, say. Hence $a_i' \ge \lceil n/p^h \rceil$ and by (11)

$$p^h a_i' = a_i \le (n-1)(a_i, a_k) = (n-1)(a_i, p^d) = (n-1)p^h,$$

thus $a_i' \le n-1$, so $a_i \in B_h$.

Case 2. $p^d | a_i$. Then $a_i = p^d a_i'$, say. Hence $a_i' \ge \lceil n/p^d \rceil$ and by the lemma $a_1 < a_k = p^d$, and by (11)

$$p^d a_i' = a_i \le (n-1)(a_i, a_1) \le (n-1)a_1 < (n-1)a_k = (n-1)p^d,$$

thus $a_i' < n-1$, so $a_i \in B_d$.

This proves the claim (12).

We define for $h = 1, \ldots, d$

$$C_h = B_h \cap A, \quad C_h' = C_h \backslash \{(n-1)p^h\}, \quad C' = \bigcup_{h=1}^{d} C_h'.$$

Let $B_0' = \{b \in B_0 : p \nmid b\}$. Define a function $f : C' \to B_0'$ in the following way:

$$x' \in C', \ x = p^t b \ (p \nmid b, \ b \le n-2) \text{ say; then } f(x) = b. \tag{13}$$

The function f is 1-1. Otherwise we have $b = b'$ for $x = p^t b$ and $x' = p^{t'} b'$ $(p \nmid bb')$. This implies $p^{t'} x = p^t x'$ which contradicts the p-simplicity of $\mathcal{A}$.

For $b \in B_0'$ there is r with $1 \le r \le p-1$ and $b \equiv r \bmod p$. Define a function $g \colon f(C') \to B_0'$ by

$$g(b) = \begin{cases} b+1 & \text{for } 2 \nmid r, \\ b-1 & \text{for } 2 \mid r. \end{cases}$$

Since $2 | (p-1)$ and $b \le n-2$ in (13) we have indeed

$$g(f(C')) \subseteq B_0'. \tag{14}$$

It is easily seen that g is 1-1:

The only interesting case is $g(b) = b+1$, $g(b') = b'-1$, $g(b) = g(b')$. This implies $b = sp + r$, $b' = s'p + r'$ with $2 \nmid r$, $2 | r'$, for some s, s', and $b + 2 = b'$. Hence $(s' - s)p = r - r' + 2$. Since $|r - r'| \le p-2$ we can have $p | (r - r' + 2)$ only for $r - r' + 2 = 0$ or $r - r' + 2 = p$. The former gives $r \equiv r' \bmod 2$, the latter $r = p - 1 \equiv 0 \bmod 2$, both contradicting the conditions on r and r'.

For $C = \bigcup_{h=1}^{d} C_h$ and $B = \{1, 2, \ldots, n-1\}$ define the function $F : C \to B$ as follows:

$$F(x) = \begin{cases} g(f(x)) & \text{for } x \in C', \\ p^h & \text{for } x = (n-1)p^h \ (p \nmid (n-1), 1 \le h \le p-1). \end{cases}$$

Indeed, $p^h \in B$, because $p^d \in B$; otherwise, since the g.c.d. of the a_i's is 1, there is a_m with $p \nmid a_m$; thus $a_k/(a_k, a_m) = p^d \ge n$ which contradicts (11). By (14) F is 1-1.

For $x \in C'$, $x = p^t b$ $(p \nmid b)$, say, we have $p \nmid F(x)$, so $(x, F(x)) = (p^t b, b \pm 1) = 1$. Since $x \in A$, $F(x)$ cannot belong to A, because $x/(x, F(x)) \ge n$ again contradicts (11). Also, the numbers p^h $(1 \le h \le d-1)$ do not belong to A, because p^d is the lowest p-power in A.

Thus we have found a 1-1 function $F : C \to B$ with $\operatorname{card}(F(C) \cup (A \cap B)) = n$; but $F(C) \cup (A \cap B) \subseteq B$. This contradiction proves the theorem.

REFERENCES

1. R. D. Boyle, *On a problem of R. L. Graham*, Acta Arith. **34** (1978), 163–177.
2. E. Z. Chein, *On a conjecture of Graham concerning a sequence of integers*, Canad. Math. Bull. **21** (1978), 285–287.
3. P. Erdös, *Problems and results on combinatorial number theory*, A Survey on Combinatorial Theory, North-Holland, Amsterdam, 1973, Chapter 12.
4. R. L. Graham, *Unsolved problem* 5749, Amer. Math. Monthly **77** (1970), 775.
5. R. Klein, *The proof of a conjecture of Graham for sequences containing primes*, Proc. Amer. Math. Soc. **95** (1985), 189–190.
6. J. Marica and J. Schönheim, *Differences of sets and a problem of Graham*, Canad. Math. Bull. **12** (1969), 635–637.
7. R. J. Simpson, *On a conjecture of R. L. Graham*, Acta Arith. **40** (1982), 209–211.
8. W. Y. Vélez, *Some remarks on a number theoretic problem of Graham*, Acta Arith. **32** (1977), 233–238.
9. G. Weinstein, *On a conjecture of Graham concerning greatest common divisors*, Proc. Amer. Math. Soc. **63** (1977), 33–38.
10. R. Winterle, *A problem of R. L. Graham in combinatorial number theory*, Proc. Louisiana Conf. on Combinatorics, Graph Theory and Computing, Louisiana State Univ., Baton Rouge, La., 1970, pp. 357–361.

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT HANNOVER, WELFENGARTEN 1, 3000 HANNOVER 1, FEDERAL REPUBLIC OF GERMANY